

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF ARIZONA

CR 05-1049-TUC-FRZ (GEE)

**REPORT AND RECOMMENDATION**

Andrew Edward Flyer,  
Defendant.

Pending before the court is the defendant's motion to dismiss superceding indictment, suppress evidence collected pursuant to a search warrant, and hold a *Franks*<sup>1</sup> hearing. [doc. ## 96, 118] The government filed a response and a supplement. [doc. ## 102, 119]

That portion of the motion addressing count 5 is now moot. The court orally granted the government's motion to dismiss that count. The Magistrate-Judge recommends the remainder of the motion be denied on the merits.

<sup>1</sup> *Franks v. Delaware*, 438 U.S. 154 (1978).

1 **CHARGES:**

2 In Count 1 of the superceding indictment, Flyer is charged with attempted  
3 transportation and shipping of child pornography in violation of 18 U.S.C. § 2252(a)(1) and  
4 (b)(1). Specifically, he is charged with attempted transmission of a computer image entitled  
5 "0-KIDDY-PTHC bw 025.jpg" on or about March 9, 2004.

6 In Count 2, Flyer is charged with attempted transportation and shipping of child  
7 pornography in violation of 18 U.S.C. § 2252(a)(1) and (b)(1). Specifically, he is charged  
8 with attempted transmission of a computer image entitled "2 Preteen Boys Fucking In The  
9 Bathtub (Gay Kiddy Porn) (3).jpg" on or about March 10, 2004.

10 In Count 3, Flyer is charged with possession of child pornography in violation of 18  
11 U.S.C. § 2252(a)(4)(B) and (b)(2). The indictment specifically names 8 computer files  
12 contained in his Gateway desktop computer on or about April 13, 2004.

13 In Count 4, Flyer is charged with possession of child pornography in violation of 18  
14 U.S.C. § 2252(a)(4)(B) and (b)(2). The indictment specifically names 21 computer files  
15 contained on disks and various storage media on or about April 13, 2004. One of the named  
16 computer files is "0-KIDDY-PTHC bw 025.jpg"

17 In Count 5, Flyer is charged with possession of child pornography in violation of 18  
18 U.S.C. § 2252(a)(4)(B) and (b)(2). The indictment specifically names 6 computer files  
19 contained in his Apple Laptop computer on or about April 13, 2004.

20  
21 **Facts:**

22 The government alleges the following facts: On or about March 9, 2004, Agent  
23 Andrews of the FBI was acting in an undercover capacity on the internet and launched file  
24 sharing software "LimeWire." She searched the network for someone offering child  
25 pornography by using the search term, "PTHC." (Defendant's motion, Exhibit 1, ¶ 32.)  
26 Agent Andrews discovered an individual with internet protocol address 68.231.131.248 who  
27 was offering several such items. *Id.* Andrews downloaded a computer image entitled "0-  
28

1 KIDDY-PTHC bw 025.jpg” from this address. *Id.* To allow this image to be transmitted,  
2 the sender must turn on his computer, run the LimeWire software program, and place this file  
3 in a special “shared” file folder. Andrews attempted to download further images but was  
4 unable to do so. *Id.*, ¶ 33. The LimeWire program printed the following message: Need  
5 More Sources. *Id.* According to Andrews, this message means too many people are  
6 requesting files from this address. *Id.*

7 On March 10, 2004, Andrews continued her investigation. *Id.*, ¶ 36. She found the  
8 individual with internet protocol address 68.231.131.248 was again offering several items.  
9 *Id.* Andrews downloaded a computer image entitled “2 Preteen Boys Fucking In The  
10 Bathtub (Gay Kiddy Porn) (3).jpg” from this address. *Id.* Andrews attempted to download  
11 further images but was unable to do so. The LimeWire program again printed the following  
12 message: Need More Sources. *Id.*

13 Agents traced this internet address to a house in the Tucson area. Agent Andrews  
14 obtained a search warrant for that address. (Defendant’s motion, Exhibit 1.) On April 13,  
15 2004, agents executed the warrant and seized a Gateway desktop computer, an Apple Laptop  
16 computer, and 178 pieces of loose storage media. When Flyer was interviewed, he admitted  
17 he used the LimeWire program to download music and videos and “sometimes child  
18 pornography comes down.” (Government’s response, p. 2.) Flyer said he has an academic  
19 interest in the accessibility of child pornography on the internet and “wanted to see what  
20 percentage of uploads are child pornography versus adult pornography.” *Id.*, p. 3. He said  
21 “he usually deletes the child pornography that he finds on the internet and only keeps a  
22 minimal amount in the ‘LimeWire’ share folder.” *Id.*

23 On July 8, 2005, Flyer pleaded guilty to the original indictment. He later retained  
24 substitute counsel, and on October 26, 2005, the court granted his motion to withdraw his  
25 plea. On January 4, 2006, the government obtained a superseding indictment.

26 On April 2, 2007, Flyer filed the instant motion to dismiss the superseding indictment  
27 or suppress the evidence collected pursuant to the search warrant and for a *Franks* hearing.  
28

1 Flyer offers the affidavit of a computer forensics expert, Tami L. Loehrs. In her affidavit,  
2 Loehrs states she examined the electronic evidence gathered pursuant to the search warrant.  
3 She concluded the Gateway desktop computer had been properly seized and acquired  
4 pursuant to industry standards. She found a number of irregularities, however, when she  
5 examined the Apple Laptop.

6 On the Laptop, Loehrs found that over 63,000 files had been accessed on March 18,  
7 2005, approximately 11 months after it had been seized. She further found 6,100 files had  
8 been accessed and eleven files had been created on November 3, 2005, approximately 19  
9 months after it had been seized.

10 Loehrs searched the Laptop for the two files that constitute counts 1 and 2 of the  
11 superseding indictment. She found both files. They listed creations dates of March 8, 2004  
12 at 3:08:40 a.m. and 3:08:44 a.m., respectively. Loehrs found it implausible that these two  
13 files should have been created at approximately the same time. Loehrs further found these  
14 two files had been accessed on March 18, 2005, approximately 11 months after the Laptop  
15 was seized.

16 According to Loehrs, the chain of custody supplied by the government does not explain  
17 why the Laptop shows the access dates March 18, 2004, and November 3, 2005.

18 Loehrs believes the Apple Laptop was accessed by unknown persons on at least two  
19 separate occasions after it had been seized. She opines the data on the Laptop could have  
20 been "inadvertantly or intentionally changed, deleted or added." (Defendant's motion,  
21 Affidavit of Tami Loehrs, ¶ 37.) Accordingly, she concludes the data on the Laptop is  
22 "completely unreliably and unusable." *Id.*

23 On April 27, 2007, the government filed a response to the motion. The government  
24 proffered the statement of SA Meshinsky who examined the Apple Laptop. (This document  
25 was later added to the record.) [doc. # 119, Attachment 1]

26 Meshinsky reports that on November 3, 2005, he conducted a forensic examination  
27 of the Apple Laptop. He attempted to image the Laptop's hard drive, but his examining  
28

1 computer system inadvertently had the "disk arbitration" setting left on. This error created  
2 some files on the Laptop and accessed some other files. This error was not documented in  
3 his notes. (Compare Hearing Exhibit A5 with Hearing Exhibit G and doc. # 119, Attachment  
4 1)

5 Meshinsky also found the system date and time on the Laptop read 04/01/1976 and  
6 8:00 A.M. This is the default setting. Meshinsky believes the battery on the Parameter RAM  
7 failed, and this failure caused the Laptop to reset the date and time to the default setting. He  
8 also hypothesizes battery failure could have caused the March 18, 2005, access file dates to  
9 have erroneously appeared.

10 A hearing on the motion was held on the 13<sup>th</sup>, 14<sup>th</sup>, and 18<sup>th</sup> of June, 2007. The court  
11 denied the defendant's motion for a *Franks* hearing. The government orally moved to  
12 dismiss count 5 of the superseding indictment, and the court granted the motion. [doc. # 113]  
13 The court allowed the defendant to make an offer of proof, and Tami Loehrs offered expert  
14 computer forensic testimony.

15  
16 **Discussion – Franks Hearing:**

17 Under certain circumstances, a defendant may challenge the veracity of the statements  
18 contained in the affidavit that the Magistrate relied upon when he or she issued the search  
19 warrant. *Franks v. Delaware*, 438 U.S. 154 (1978). The affidavit supporting the warrant is  
20 presumed to be valid. *Id.* at 171. Accordingly, the defendant is entitled to a hearing on the  
21 issue only "if he makes a substantial preliminary showing that a false statement was  
22 deliberately or recklessly included in the search warrant affidavit and that the statement was  
23 necessary to the magistrate's finding of probable cause." *United States v. Napier*, 436 F.3d  
24 1133, 1139 (9<sup>th</sup> Cir. 2006), *cert. denied*, 127 U.S. 164 (2006).

25 Flyer maintains the files on the Apple Laptop are irretrievably compromised. The  
26 government, therefore, cannot show Flyer had the two images of child pornography on his  
27 computer when Agent Andrews said she downloaded them. He argues these images were  
28

1 not on the Apple Laptop before the search, and Agent Andrews lied when she said she  
2 downloaded them from his computer.

3 Flyer further notes that Tami Loehrs worked on two previous cases where Agent  
4 Andrews claimed she downloaded files from the defendants' computers, but the files  
5 subsequently were not found on the computers' hard drives. He further notes the computer  
6 in this case was accessed by the government on November 3, 2005, just two days after the  
7 government learned the defendant had retained Tami Loehrs. These facts, he argues, create  
8 the suspicion that the Apple Laptop was deliberately tampered with to make it appear that  
9 these two image files were on the computer when Agent Andrews said she downloaded them.

10 In this case, Flyer has not made a "substantial preliminary showing that a false  
11 statement was deliberately or recklessly included in the search warrant affidavit." *See United*  
12 *States v. Napier*, 436 F.3d 1133, 1139 (9<sup>th</sup> Cir. 2006). The Apple Laptop is no longer in the  
13 same conditions as it was when it was seized. If Loehrs is correct and the hard drive has no  
14 evidentiary value, the government cannot now show the two image files were on the Apple  
15 Laptop when Agent Andrews allegedly downloaded them. This, however, does not prove  
16 Agent Andrews lied when she said she downloaded the image files from Flyer's computer.  
17 There are many reasons why these files might not be on the Laptop on the day of the seizure.  
18 They could have been erased. When examining the Gateway desktop computer, the  
19 government found child pornography in the "DriveFreeSpace" indicating these images had  
20 been downloaded and then deleted. (Government's response, p. 3.) Flyer, himself, said he  
21 usually deletes the child pornography he finds on the internet.

22 Moreover, other evidence supports the veracity of the affidavit. Large amounts of  
23 child pornography were found in the loose storage media and on the Gateway desktop  
24 computer. Flyer admitted he downloads computer files using the LimeWire program. He  
25 further admitted he downloaded child pornography and was interested in what percentage of  
26 uploads are child pornography versus adult pornography. This evidence bolsters the  
27 presumption that the affidavit is valid, and undermines Flyer's argument. *See Napier*, 436  
28

1 F.3d at 1139 (“This presumption is bolstered, where as here, the incriminating results of the  
2 search . . . undermine [the defendant’s] offer of proof.”).

3       Flyer maintains the timing of the government’s forensic investigation, conducted on  
4 November 3, 2005, is suspicious. He offers the following hypothesis: When the government  
5 agents found out the defendant retained a computer expert, they feared she would discover  
6 the two image files were missing and decided to falsify the evidence. The court finds this  
7 scenario unlikely.

8       This case has a rather lengthy history of proceedings. Flyer was originally indicted  
9 on May 25, 2005. He pleaded guilty less than two months later. Presumably, the  
10 government hoped to resolve the case quickly without expending the time and resources  
11 necessary to image the computer and allow the defendant access to the electronic evidence.  
12 Flyer subsequently filed motions to withdraw his plea and substitute counsel which the court  
13 granted in October of 2005. The government conducted its forensic examination of the  
14 Apple Laptop in November of 2005 because the case appeared to be headed for trial and the  
15 defendant was entitled to discovery. There is no evidence the government accessed the  
16 Laptop because it was afraid the defendant’s expert would discover that the two image files  
17 were missing.

18       Flyer notes that in two earlier cases, Agent Andrews claimed she downloaded files  
19 from the defendants’ computers, but the files subsequently were not found on the computers’  
20 hard drives. He argues this fact strengthens the likelihood that evidence was falsified in this  
21 case. The court does not agree.

22       In *United States v. Ernest David Craighead*, CR 04-2351 TUC JMR, the District  
23 Court denied the defendant’s motion for a *Franks* hearing even though the government was  
24 unable to find the computer files that Agent Andrews said she downloaded from the  
25 defendant’s computer. (Government’s response, p. 9.) This case, in fact, weakens Flyer’s  
26 argument. If Agent Andrews were indeed fabricating these downloads, why would she try  
27 to falsify evidence in this particular case? In the earlier case, the smoking-gun files were  
28

1 missing from the defendant's computer, and the defendant still lost his motion for a *Franks*  
2 hearing. Presumably, she would expect the same result here: The files would be found to be  
3 missing, the defendant would file a *Franks* motion, and the court would deny the motion.  
4 This earlier case makes it *less* likely the government would attempt to falsify the evidence.  
5 There is simply no need to cheat when you expect to win as a matter of course. *See also*  
6 *United States v. Anthony David Hibble*, CR 05-1410-TUC-DCB (HCE) (Although the  
7 smoking gun files were not found on the defendant's computer, the defendant's motion for  
8 a *Franks* hearing was denied.).

9 In the alternative, Flyer argues the time and date information attached to the two  
10 image files is valid and the creation dates of the two files are suspiciously similar. These two  
11 files have creation dates of March 8, 2004 at 3:08:40 and 3:08:44 a.m. respectively. Agent  
12 Andrews claims she downloaded one on March 9, 2004 and the other on March 10, 2004.  
13 Flyer argues that because Agent Andrews had hundreds of possible files to chose from on  
14 March 10, 2004, it is unlikely she would choose a file that was created within four seconds  
15 of the file she chose to download the previous day.

16 This argument is undercut by Flyer's main argument. The Apple Laptop was  
17 inadvertently accessed and is no longer in the same condition as it was on the day it was  
18 seized. These creation times are therefore suspect.

19 Assuming the creation information is correct, Flyer cannot show it is unlikely the two  
20 files would have similar creation times. Apparently, Loehrs assumes Agent Andrews  
21 downloaded these two files at random from the scores of files she located using the search  
22 term, "PTHC." If Andrews did indeed do this, then it would be unlikely that she would  
23 download two files with similar creation times. The affidavit, however, does not say this.  
24 (Defendant's motion, Exhibit 1.) It says, Andrews found and downloaded a file located using  
25 the search term, "PTHC," from IP address 68.231.131.248. *Id.*, ¶ 32. The next day, she  
26 found additional files using the search term, "PTHC." *Id.*, ¶ 36. She again found many such  
27 files available from IP address 68.231.131.248. *Id.* She then downloaded the second image  
28



1 file from that address. *Id.* She does not say the second image file was among those files she  
2 found using the search term, “PTHC.”

3 The second file was not chosen at random. It was chosen from the group of files  
4 offered by IP address 68.231.131.248 on March 10, 2004 – the same IP address, presumably  
5 the same computer, that offered the first image file. It is one thing to say two files of child  
6 pornography chosen at random from all the LimeWire files offered on two successive days  
7 probably would not have the same creation times. It is quite another to say two files of child  
8 pornography offered *from the same IP address* on two successive days would not have the  
9 same creation times. It is possible these two files were copied by Flyer at the same time. The  
10 defendant provides no evidence to discount this possibility.

11 Flyer has not made a “substantial preliminary showing” that Agent Andrews lied when  
12 she stated she downloaded two images of child pornography from Flyer’s computer. *See*  
13 *United States v. Napier*, 436 F.3d 1133, 1139 (9<sup>th</sup> Cir. 2006). His request for a *Franks*  
14 hearing should be denied.

15 Flyer further argues Andrews was intentionally misleading when she said in the  
16 affidavit she was unable to download further files because too many other users were trying  
17 to copy Flyer’s files. Flyer maintains there are many other possible reasons why LimeWire  
18 would print the message, “Need More Sources.”

19 Andrews’ statement, however, was not necessary to the magistrate’s finding of  
20 probable cause. *See United States v. Napier*, 436 F.3d 1133, 1139 (9<sup>th</sup> Cir. 2006).  
21 Accordingly, Flyer is not entitled to a *Franks* hearing even if it was intentionally misleading.

22  
23 **Discussion – Due Process:**

24 Flyer further moves that this court dismiss the superseding indictment or suppress the  
25 evidence obtained from the search because potentially exculpatory information was destroyed  
26 by the government.

1 The government's failure to preserve evidence violates the defendant's right to due  
2 process right if "the unavailable evidence possessed exculpatory value that was apparent  
3 before the evidence was destroyed, and is of such a nature that the defendant would be  
4 unable to obtain comparable evidence by other reasonably available means." *United States*  
5 *v. Cooper*, 983 F.2d 928, 931 (9<sup>th</sup> Cir. 1993). Due process is violated only if the government  
6 acted in bad faith. *Id.* The defendant's task of proving bad faith is problematic if the  
7 exculpatory value was not apparent before the evidence was destroyed. If the defendant's  
8 due process rights are so violated, the court may dismiss the indictment against him. *Id.* at  
9 933.

10 In this case, there is no evidence the alleged exculpatory value of the Apple Laptop  
11 was apparent when it was accessed by the government. Flyer admitted to the agents that he  
12 used the LimeWire program and downloaded pornography. There is no evidence the  
13 government believed the Laptop would have any exculpatory value, e.g., no evidence the  
14 government believed the two image files would be absent from Flyer's computer. Because  
15 the alleged exculpatory value of the Laptop was not apparent, Flyer cannot show the  
16 government destroyed evidence in bad faith. Flyer's due process rights were not violated,  
17 and the indictment should not be dismissed.

18  
19 **Discussion – Suppression:**

20 If the government destroys evidence under circumstances that do not violate the  
21 defendant's constitutional rights, the court may still issue a protective order or impose  
22 sanctions including suppression of secondary evidence. *United States v. Loud Hawk*, 628  
23 F.2d 1139, 1152 (9<sup>th</sup> Cir. 1979) (en banc) (Kennedy, J., concurring), *cert. denied*, 445 U.S.  
24 917 (1980). The court must balance "the quality of the Government's conduct and the degree  
25 of prejudice to the accused." *Id.* "The Government bears the burden of justifying its conduct  
26 and the defendant bears the burden of demonstrating prejudice." *Id.*

1        “In weighing the conduct of the Government, the court should inquire whether the  
2 evidence was lost or destroyed while in its custody, whether the Government acted in  
3 disregard for the interests of the accused, whether it was negligent in failing to adhere to  
4 established and reasonable standards of care for police and prosecutorial functions, and, if  
5 the acts were deliberate, whether they were taken in good faith or with reasonable  
6 justification.” *Id.* “It is relevant also to inquire whether the government attorneys prosecuting  
7 the case have participated in the events leading to loss or destruction of the evidence, for  
8 prosecutorial action may bear upon existence of a motive to harm the accused.” *Id.*

9        “In analyzing prejudice, the court must consider a wide number of factors including,  
10 without limitation, the centrality of the evidence to the case and its importance in establishing  
11 the elements of the crime or the motive or intent of the defendant; the probative value and  
12 reliability of the secondary or substitute evidence; the nature and probable weight of factual  
13 inferences or other demonstrations and kinds of proof allegedly lost to the accused; the  
14 probable effect on the jury from absence of the evidence, including dangers of unfounded  
15 speculation and bias that might result to the defendant if adequate presentation of the case  
16 requires explanation about the missing evidence.” *Id.*

17        In this case, the Laptop was in the government’s custody when it was altered. The  
18 government agents were negligent in their handling of the evidence. There is, however, no  
19 evidence the government acted in bad faith or that government attorneys prosecuting the case  
20 were involved in the loss of evidence.

21        The Laptop is of some importance to counts one and two. (It is of central importance  
22 to count five, but this count has been dismissed.) If the two image files were not on the  
23 Laptop and the Laptop were unaltered, this would be some evidence that Flyer did not  
24 attempt to transmit them over the internet. The remainder of the evidence, however, weighs  
25 against this possible defense. Large amounts of child pornography was found in Flyer’s  
26 possession. He admitted he used LimeWire to transfer files such as child pornography. In  
27 fact, one of the two image files he allegedly attempted to transport, “0-KIDDY-PTHC bw  
28

1 025.jpg," was found in the loose storage media. [doc. # 31] Moreover, Flyer said he deleted  
2 most of the child pornography that he downloaded. This evidence tends to prove that Flyer  
3 attempted to transport these two image files in March of 2004 and supplies an explanation  
4 for why they might not be found on the Laptop at the time of the seizure. In sum, Flyer  
5 cannot show the government's destruction of evidence has significantly affect his ability to  
6 present an effective defense.

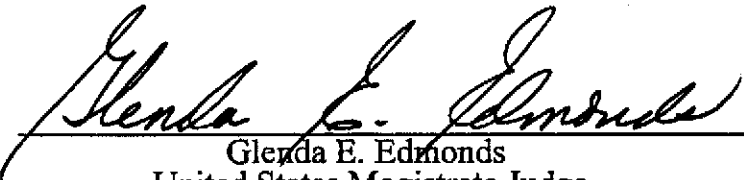
7 The government has been negligent, but Flyer has not been significantly prejudiced.  
8 Flyer's motion for sanctions should be denied. If the government introduces evidence that  
9 the two image files were found on the Laptop, the defendant should be able to effectively  
10 dispute the reliability of that evidence.

11  
12 **RECOMMENDATION:**

13 In view of the foregoing, it is recommended that after an independent review of the  
14 record, the District Court should **DENY** the defendant's motion to dismiss the superceding  
15 indictment, suppress evidence collected pursuant to a search warrant, and hold a *Franks*  
16 hearing. [doc. ## 96, 118] The defendant's motion to dismiss count 5 is now moot. The  
17 remainder of the motion should be denied on the merits.

18 This Report and Recommendation is being faxed to all counsel on this date. Counsel  
19 must file any objections within ten (10) days of today's date.

20  
21 DATED this 13<sup>th</sup> day of July, 2007.

22  
23  
24   
25 Glenda E. Edmonds  
26 United States Magistrate Judge  
27  
28